CLAIMS

What is claimed is:

1. A method for on-access computer virus scanning of files in an efficient manner, comprising the steps of:

(a) identifying a process for accessing files;

(b) selecting virus detection actions based at least in part on the process; and

(c) performing the virus detection actions on the files.

2. The method as recited in claim 1, wherein the process is carried out by an executable file.

3. The method as recited in claim 1, wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category.

4. The method as recited in claim 1, and further comprising the steps of identifying the files being accessed, and selecting the virus detection actions based at least in part on the identity of the files.

5. The method as recited in claim 1, wherein the process is identified by inspecting at least one of a name of the process, a path of the process, a file signature associated with the process, a version of the process, a manufacturer of the process, a function being called during the process, an owner of the process, a name of an executable file associated with the process, a method in which files are being accessed by the process, type(s) of shared libraries used by the identified process, and a user of the process.

6. The method as recited in claim 1, wherein no virus detection actions are selected upon the identification of a predetermined process.

7. A computer program product for on-access computer virus scanning of files in an efficient manner, comprising:
(a) computer code for identifying a process for accessing files;
(b) computer code for selecting virus detection actions based at least in part on the process; and
(c) computer code for performing the virus detection actions on the files.

8. The computer program product as recited in claim 7, wherein the process is carried out by an executable file.

9. The computer program product as recited in claim 7, wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category.

10. The computer program product as recited in claim 7, and further comprising computer code for identifying the files being accessed, and selecting the virus detection actions based at least in part on the identity of the files.

11. The computer program product as recited in claim 7, wherein the process is identified by inspecting at least one of a name of the process, a path of the process, a file signature associated with the process, a version of the process, a manufacturer of the process, a function being called during the process, an owner of the process, a name of an executable file associated with the process, a method in which files are being accessed by the process, type(s) of shared libraries used by the process, and a user of the process.

12. The computer program product as recited in claim 7, wherein no virus detection actions are selected upon the identification of a predetermined process.

13. A system for on-access computer virus scanning of files in an efficient manner, comprising:
(a) logic for identifying a process for accessing files;
(b) logic for selecting virus detection actions based at least in part on the process; and
(c) logic for performing the virus detection actions on the files.

14. The system as recited in claim 13, wherein the process is carried out by an executable file.

15. The system as recited in claim 13, wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category.

16. The system as recited in claim 13, and further comprising logic for identifying the files being accessed, and selecting the virus detection actions based at least in part on the identity of the files.

17. The system as recited in claim 13, wherein the process is identified by inspecting at least one of a name of the process, a path of the process, a file signature associated with the process, a version of the process, a manufacturer of the process, a function being called during the process, an owner of the process, a name of an executable file associated with the process, a method in which files are being accessed by the process, type(s) of shared libraries used by the process, and a user of the process.

18. The system as recited in claim 13, wherein no virus detection actions are selected upon the identification of a predetermined process.

19. A method for on-access computer virus scanning of files of a system in an efficient manner, comprising the steps of:
(a) identifying a first aspect of the system;
(b) identifying a second aspect of the system;
(c) selecting virus detection actions based at least in part on the first aspect of the system and at least in part on the second aspect of the system; and
(d) performing the virus detection actions on the files.

20. The method as recited in claim 19, wherein the first aspect of the system includes a process adapted for accessing the files, and the second aspect of the system includes a type of the files.

21. A computer program product for on-access computer virus scanning of files of a system in an efficient manner, comprising:
(a) computer code for identifying a first aspect of the system;
(b) computer code for identifying a second aspect of the system;
(c) computer code for selecting virus detection actions based at least in part on the first aspect of the system and at least in part on the second aspect of the system; and
(d) computer code for performing the virus detection actions on the files.